IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP AF**
Martin Naedele et al.	Group Art Unit: 2431
Application No.: 10/582,633	Examiner: Brett S Squires
Filed: June 12, 2006	Confirmation No.: 2009
For: IT NETWORK SECURITY SYSTEM	

REQUEST FOR PRE-APPEAL BRIEF CONFERENCE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants request that the May 21, 2009 final rejection of Claims 1-18 in the above-identified application be reviewed and withdrawn for the following reasons.

1. The Examiner has committed clear error by rejecting independent claim 1 under 35 U.S.C. § 102(e) because Nazzal (US PG Pub 2004/0261030) fails to anticipate Applicants' claim 1 features of a **data source** with means for **generating network-security relevant data** and a processing module with means for **translating said network security relevant data into quantitative variables.**

2. The Examiner has committed clear error in rejecting Applicants' depending claims under 35 U.S.C. § 103(a) when none of the documents relied upon disclose or suggest Applicants' claimed **data source** and/or **translating** features.

Argument

Exemplary embodiments are directed to a network security system for detecting security irregularities in a network, and, as shown in Fig. 3, include "data sources" located on or constituting the network. The **data sources** include means for **generating data that is network-security relevant data.** For example, network-security relevant data can be traffic rates generated by a Linux host configured as a router or a Cisco Catalyst 2926 switch, selected messages from a Windows 2000 event log converted to Syslog via intersect Alliance SNARE, and/or the alert firing rate of a Snort IDS (Intrusion Detection System) with the Spade statistical IDS. See, for example, page 8, 3rd paragraph of Applicants' specification. Exemplary embodiments of the network security system shown in Fig. 3 include an "input" module with input handlers for various protocols (e.g. SNMP or syslog) to connect to the data sources.

In the exemplary embodiments, at least one processing module is connected to the input module for access to the data sources, and includes means for **translating network security relevant data** into quantitative variables. A supervisory system can present the quantitative variables to a security system operator. Such quantitative information can enable a human process operator to make decisions as to the severity of an overall situation on the network. Such an exemplary network security system presents quantitative variables for the human process operator to detect and act upon network security issues based on the displayed quantitative variables.

The Nazzal document is fundamentally different from Applicants' presently disclosed embodiments, and these differences are reflected in Applicants' claim 1.

Nazzal's system includes a network which serves as a conduit for network data forwarded by switches and/or routers. The switches and routers themselves do not **generate network security relevant data.**

Nazzal discloses an anomaly detection system 10 that relies on a number of collectors 12 to monitor a network 18 and send reports to an aggregator 14. See paragraphs 44 and 45 of Nazzal. The Examiner cites network devices (e.g. switches 15) of Nazal as allegedly corresponding to Applicants' claim 1 data sources. However, the network devices of Nazal do not include means for generating network-security relevant data, as recited in Applicants' claim 1. The switches 15 in Nazzal route **traffic** but do not generate network security relevant data. The traffic in a network cannot constitute network-security relevant data, as recited in Applicants' claim 1, because the traffic does not constitute information related to network security.

The Examiner cites the collectors 12 of Nazzal as allegedly corresponding to Applicants' claim 1 "input modules." The Examiner cites aggregator 14 of Nazzal as allegedly corresponding to Applicants' claim 1 processing module with means for "translating" network-security relevant data into quantitative variables. However, because Nazzal's approach and problems addressed are fundamentally different from those of the present application, aggregator 14 of Nazzal does not translate traffic into quantitative variables. In Nazzal, the traffic is sampled by the collectors 12, and the collectors 12 provide data—not traffic— to the aggregator 14. Because the aggregator 14 does not **translate the traffic** into quantitative variables, Nazzal does not disclose the at least one "processing module", as recited in Applicants' claim 1.

The Symantec publication, Bhattacharya (US PG Pub 2005/0060562), and Rangachari (US PG Pub 2003/0176940) do not cure the deficiencies of Nazzal. As such, none of the documents relied upon by the Examiner, considered individually or in the combination set forth by the Examiner, disclose the features of Applicants' claim 1.

For example, the Symantec publication relates to suspicious activity alerts via an alert box as shown in Fig. 4-6, and was applied in combination by the Examiner to reject dependent claim 4, which provides for reaction facilities with means for initiating predefined countermeasures. The Symantec publication relates to virus alerts on a single system and does not suggest any application to network security analysis and response to network security events.

Rangachari describes an automation system for a semiconductor fabrication plant, but does not disclose the above network security system features for detecting security relevant irregularities as in Applicants' claim 1.

As such, Applicants' claim 1 is allowable, as are all dependent claims. See, for example, dependent claims 3 and 4 which recite features of network-security relevant data and means for initiating predefined countermeasures.

Conclusion

In view of the foregoing, withdrawal of the rejections is respectfully requested, along with a Notice of Allowance.

In the event that there are any questions, the Examiner is respectfully requested to telephone the undersigned so that prosecution of present application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: August 21, 2009 By: Michael Weinberg #63985

Patrick C. Keane
Registration No. 32858

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620